

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

SUBJECT STORAGE UNIT:  
Located at 4020 Leary Way N, Seattle, WA 98107,  
Unit 129

Case No. MJ20-120

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)	Possession of Controlled Substance with Intent to Distribute

The application is based on these facts:

- ☒ See Affidavit of HSI Special Agent Ernest McGeachy.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

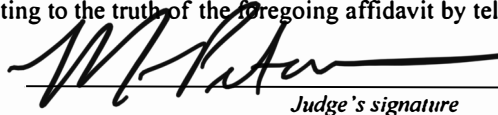
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

  
Applicant's signature

SA Ernest McGeachy, HSI  
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/12/2020

  
Judge's signature

City and state: Seattle, Washington

Hon. Michelle L. Peterson, U.S. Magistrate Judge  
Printed name and title

**ATTACHMENT A**

**Place to Be Searched**

The place to be searched is 4020 Leary Way NW, Unit 129, Seattle, WA 98107 (the “**SUBJECT STORAGE UNIT**”), a single storage unit located first floor of the building. The storage unit has a gray door with a front window.



**ATTACHMENT B**

**List of Items to be Seized**

Evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Distribution of and Possession of, with Intent to Distribute, Controlled Substances), committed by Tristan BRENNAND and his co-conspirator(s), as follows:

1. Controlled Substances: Including but not limited to heroin, methamphetamine, and cocaine;

2. Drug Paraphernalia: Items used, or to be used, to store, process, package, use, and/or distribute controlled substances, such as plastic bags, DVD cases, cutting agents, scales, measuring equipment, vials, pill presses, Mylar bags, heat/vacuum sealers, tape, duffel bags, chemicals or items used to test the purity and/or quality of controlled substances, and similar items;

3. Drug Transaction Records: Documents such as ledgers, receipts, notes, and similar items relating to the acquisition, transportation, and distribution of controlled substances;

4. Customer and Supplier Information: Items identifying drug customers and drug suppliers, such as telephone records, personal address books, correspondence, diaries, calendars, notes with phone numbers and names, "pay/owe" sheets with drug amounts and prices, maps or directions, and similar items;

5. Cash and Financial Records: Currency and financial records, including bank records, safe deposit box records and keys, credit card records, bills, receipts, tax returns, vehicle documents, and similar items; and other records that show income and expenditures, net worth, money transfers, wire transmittals, negotiable instruments, bank drafts, cashier's checks, and similar items, and money counters;

6. Photographs/Surveillance: Photographs, video tapes, digital cameras, surveillance cameras and associated hardware/storage devices, and similar items, depicting property occupants, friends and relatives of the property occupants, or suspected buyers or sellers of controlled substances, controlled substances or other contraband, weapons, and assets derived from the distribution of controlled substances;

7. Weapons: Including firearms, magazines, ammunition, and body armor;

1        8.        Codes: Evidence of codes used in the distribution of controlled substances,  
2 including passwords, code books, cypher or decryption keys, usernames and/or  
3 credentials for dark web marketplaces, and similar information;

4        9.        Property Records: Deeds, contracts, escrow documents, mortgage  
5 documents, rental documents, and other evidence relating to the purchase, ownership,  
6 rental, income, expenses, or control of the premises, and similar records of other property  
7 owned or rented;

8        10.       Indicia of occupancy, residency, and/or ownership of assets including,  
9 utility and telephone bills, canceled envelopes, rental records or payment receipts, leases,  
10 mortgage statements, and other documents;

11       11.       Evidence of Storage Unit Rental or Access: Rental and payment records,  
12 keys and codes, pamphlets, contracts, contact information, directions, passwords or other  
13 documents relating to storage units;

14       12.       Evidence of Personal Property Ownership: Registration information,  
15 ownership documents, or other evidence of ownership of property including, but not  
16 limited to vehicles, vessels, boats, airplanes, jet skis, all-terrain vehicles, RVs, and  
17 personal property; evidence of international or domestic travel, hotel/motel stays, and any  
18 other evidence of unexplained wealth;

19       13.       Individual and business financial books, records, receipts, notes, ledgers,  
20 diaries, journals, and all records relating to income, profit, expenditures, or losses, such  
21 as:

22           b.       Employment records: paychecks or stubs, lists and accounts of  
23 employee payrolls, records of employment tax withholdings and  
24 contributions, dividends, stock certificates, and compensation to  
25 officers.

26           c.       Savings accounts: statements, ledger cards, deposit tickets, register  
27 records, wire transfer records, correspondence, and withdrawal slips.

28           d.       Checking accounts: statements, canceled checks, deposit tickets,  
credit/debit documents, wire transfer documents, correspondence, and  
register records.

          e.       Loan Accounts: financial statements and loan applications for all loans  
applied for, notes, loan repayment records, and mortgage loan records.

          f.       Collection accounts: statements and other records.

- g. Certificates of deposit: applications, purchase documents, and statements of accounts.
- h. Credit card accounts: credit cards, monthly statements, and receipts of use.
- i. Receipts and records related to gambling wins and losses, or any other contest winnings.
- j. Insurance: policies, statements, bills, and claim-related documents.
- k. Financial records: profit and loss statements, financial statements, receipts, balance sheets, accounting work papers, any receipts showing purchases made, both business and personal, receipts showing charitable contributions, and income and expense ledgers.

14. All bearer bonds, letters of credit, money drafts, money orders, cashier's checks, travelers checks, Treasury checks, bank checks, passbooks, bank drafts, money wrappers, stored value cards, and other forms of financial remuneration evidencing the obtaining, secreting, transfer, and/or concealment of assets and/or expenditures of money;

15. All Western Union and/or Money Gram documents and other documents evidencing domestic or international wire transfers, money orders, official checks, cashier's checks, or other negotiable interests that can be purchased with cash, to include applications, payment records, money orders, frequent customer cards, etc;

16. Negotiable instruments, jewelry, precious metals, financial instruments, and other negotiable instruments;

17. Documents reflecting the source, receipt, transfer, control, ownership, and disposition of United States and/or foreign currency;

18. Correspondence, papers, records, and any other items showing employment or lack of employment;

19. Telephone books, and/or address books, facsimile machines, any papers reflecting names, addresses, telephone numbers, pager numbers, cellular telephone numbers, facsimile, and/or telex numbers, telephone records and bills relating to co-conspirators, sources of supply, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists. Also, telephone answering devices that record telephone conversations and the tapes therein for messages left for or by co-

1 conspirators for the delivery or purchase of controlled substances or laundering of drug  
2 proceeds;

3 20. Safes and locked storage containers, and the contents thereof which are  
4 otherwise described in this document;

5 21. Tools: Tools that may be used to open hidden compartments in vehicles,  
6 paint, bonding agents, magnets, or other items that may be used to open/close said  
7 compartments;

8 22. Any and all mailing documents and packaging materials related to U.S.  
9 Postal Service to include USPS Express Mail labels, express mail and priority envelopes,  
10 first class mailings, receipts for USPS packages, and tracking information;

11 23. Any records or information pertaining to the dark web and dark web  
12 marketplaces, including the Empire Market.

13 24. Any records or information pertaining to the Subject Moniker (or spelling  
14 variants thereof);

15 25. Cryptocurrency applications and wallets, to include information regarding  
16 current account balance and transaction history, i.e., date, time, amount, an address of the  
17 sender/recipient of a cryptocurrency transaction maintained in such wallets;

18 26. Any records or information reflecting cryptocurrencies, including web  
19 history, and documents showing the location, source, and timing of acquisition of any  
20 cryptocurrencies, to include wallets, wallet addresses, and seed phrases;

21 27. Any evidence of cryptocurrency ownership or usage, to include the  
22 following: (a) any and all representations of cryptocurrency public keys or addresses,  
23 whether in electronic or physical format; (b) any and all representations of  
24 cryptocurrency private keys, whether in electronic or physical format; and (c) any and all  
25 representations of cryptocurrency wallets or their constitutive parts, whether in electronic  
26 or physical format, to include "recovery seeds" and "root keys" which may be used to  
27 regenerate a wallet.

28 28. Cell Phones: Cellular telephones and other communications devices may be  
seized, and searched for the following items:

- a. Assigned number and identifying telephone serial number (ESN, MIN,  
IMSI, or IMEI);



- b. Stored list of recent received, sent, and missed calls;
- c. Stored contact information;
- d. Stored photographs of narcotics, currency, firearms or other weapons, evidence of suspected criminal activity, and/or the user of the phone and/or co-conspirators, including any embedded GPS data associated with these photographs;
- e. Stored text messages, as well as any messages in any internet messaging apps, including but not limited to Facebook Messenger, iMessage, Wickr, Telegram, Signal, WhatsApp, Kik, and similar messaging applications, related to the aforementioned crimes of investigation or that may show the user of the phone and/or co-conspirators, including Apple iMessages, Blackberry Messenger messages or other similar messaging services where the data is stored on the telephone;
- f. Any Tor applications and records for Tor activity, including browser history and “bookmarked” or “favorite” web pages;
- g. Digital currency applications and wallets, to include information regarding current account balance and transaction history, i.e., date, time, amount, an address of the sender/recipient of a digital currency transaction maintained in such wallets;
- h. Stored documents, notes, and files that contain passwords/or encryption keys;
- i. PGP applications, to include stored private and/or public keys;
- j. Any records or information related to the use of the Subject Moniker (or spelling variants thereof); and

29. Digital devices, such as computers, and other electronic storage media, such as USBs and Trezor devices, may be seized, and searched for the following items:

- a. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

1 browsing history, user profiles, e-mail, e-mail contacts, "chats,"  
2 instant messaging logs, photographs, and correspondence;

3 b. Evidence of the attachment to the digital device of other storage  
4 devices or similar containers for electronic evidence;

5 c. Evidence of counter-forensic programs (and associated data) that are  
6 designed to eliminate data from the digital device or other electronic  
7 storage media;

8 d. Evidence of the times the digital device or other electronic storage  
9 media was used;

10 e. Passwords, encryption keys, and other access devices that may be  
11 necessary to access the digital device or other electronic storage  
12 media;

13 f. Contextual information necessary to understand the evidence  
14 described in this attachment;

15 g. Records or information pertaining to the dark web and dark web  
16 marketplaces, including the Empire Market.

17 h. Any records or information pertaining to the Subject Moniker (or  
18 spelling variants thereof);

19 i. Any records or information pertaining to Tor;

20 j. Any records or information pertaining to mnemonic phrases;

21 k. Any records or information reflecting cryptocurrencies, including  
22 web history, and documents showing the location, source, and  
23 timing of acquisition of any cryptocurrencies, to include wallets,  
24 wallet addresses, and seed phrases;

25 l. Any records or information pertaining to PGP applications, to  
26 include private and/or public keys;

27 THE SEIZURE OF DIGITAL DEVICES IS AUTHORIZED FOR THE PURPOSE OF  
28 CONDUCTING OFF-SITE EXAMINATION OF THEIR CONTENTS FOR



1 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED  
2 CRIMES  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# AFFIDAVIT OF ERNEST MCGEACHY

STATE OF WASHINGTON           )  
   )          SS  
COUNTY OF KING               )

I, ERNEST MCGEACHY, being first duly sworn on oath, hereby depose and state as follows:

## INTRODUCTION

1. I am a Special Agent (SA) with the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge (SAC), Seattle, Washington. I have been a special agent with HSI since October 2010. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. As part of my duties, I investigate criminal violations relating to cybercrimes on the Dark Web, narcotics, and financial. I have investigated and/or participated in many federal criminal investigations involving narcotics, financial and cybercrimes on the Dark Net.

2. I am a graduate of the Federal Law Enforcement Training Center (FLETC) Basic Criminal Investigator Training Program, the Immigration and Customs Special Agent Training Program, and the Naval Criminal Investigative Service (NCIS) Special Agent Training Program. Before joining HSI, I worked as a special agent with NCIS, and as a Customs and Border Protection officer. I hold a bachelor's degree in Political Science from Western Washington University. I also hold a master's degree in Human Relations from the University of Oklahoma. Additionally, I have attended HSI's Advanced Darknet and Cryptocurrency course.

//  
//  
//

**PURPOSE OF AFFIDAVIT**

3. I make this affidavit in support of an application for a search warrant authorizing the search of the following location:

a. 4020 Leary Way NW, Storage Unit 129, Seattle, WA 98107  
(hereinafter the “**SUBJECT STORAGE UNIT**”), further described in Attachment A, which is incorporated herein by reference;

4. As set forth below, there is probable cause to believe that the **SUBJECT STORAGE UNIT** will contain or possess evidence, fruits, and instrumentalities of possession of controlled substances with intent to distribute, and distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a). I seek authorization to search and seize the items specified in Attachment B, which is incorporated herein by reference.

5. The facts in this affidavit come from my personal observations, my training an experience, and information obtained from other agents and witnesses. I have not included every fact known concerning this investigation. I have set forth the facts that I believe are necessary for a fair determination of probable cause for the requested search warrant. When the statements of others are set forth in this affidavit, they are set forth in substance and in part.

6. I am familiar with the information contained in the Affidavit based upon the investigation that I have conducted, my conversations with other law enforcement officers who have engaged in various aspects of this investigation, and based upon my review of reports written by other law enforcement officers involved in this investigation. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are relevant to determination of probable cause to support the issuance of the requested warrant. When the statements of others are set forth in this Affidavit, they are set forth in substance and in part.

**BACKGROUND ON THE DARK WEB**

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions.

8. The “dark web” is a portion of the “Deep Web” of the Internet, where individuals must use anonymizing software or applications to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the “clear web” or simply the “web”). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces, also called Hidden Services, such as Silk Road, operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. There are a number of marketplaces that have appeared on the dark web that have offered contraband for sale, including narcotics. Users typically purchase narcotics through these marketplaces using virtual currency such as bitcoins.<sup>1</sup>

9. “Vendors” are the dark web’s sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of “vendor accounts” on dark web marketplaces. Customers, meanwhile, operate “customer accounts.” Vendor and customer accounts are not identified by numbers, but rather monikers or “handles,” much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces. Based on customer reviews, vendors can become well known as “trusted” vendors.

---

<sup>1</sup> Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) or “BTC” to label units of the cryptocurrency. That practice is adopted here.

1           10.    Pretty Good Privacy (“PGP”) is used on dark web markets to encrypt  
2 communications between vendors and customers. When a customer orders from a  
3 vendor or sends a vendor a message on a dark web market, that information may be  
4 stored in the marketplace’s database. The marketplace server may be hacked or seized by  
5 law enforcement, and a customer may not want their private messages with any sensitive  
6 information, like name and address, easily viewable by anyone who obtains access to the  
7 database. These messages may also be seen by someone who has access to the vendor’s  
8 computer or market account, such as a market administrator. PGP encryption is used to  
9 solve this problem.

10           11.    A vendor has both a PGP private key and a public key. A customer can use  
11 the vendor’s public key to encrypt a message. The vendor then uses their private key to  
12 decrypt the message. Vendors keep their private key secure but not their public key,  
13 which they put on their profile. This is done so customers may use a vendor’s PGP  
14 public key to encrypt data sent to the vendor, such as the customer’s name and address.  
15 Only the corresponding PGP private key, held by the vendor, can decrypt the data.

16           12.    The Onion Router or “Tor” network is a special network of computers on  
17 the Internet, distributed around the world, that is designed to conceal the true Internet  
18 Protocol (“IP”) addresses of the computers accessing the network, and thereby the  
19 locations and identities of the network’s users. Tor likewise enables websites to operate  
20 on the network in a way that conceals the true IP addresses of the computer servers  
21 hosting the websites, which are referred to as “hidden services” on the Tor network.  
22 Such “hidden services” operating on Tor have complex web addresses, which are many  
23 times generated by a computer algorithm, ending in “.onion” and can only be accessed  
24 through specific web browser software designed to access the Tor network. Most  
25 “hidden services” are considered dark web services with no legitimate or identified  
26 service provider to which legal process may be served.

**BACKGROUND ON CRYPTOCURRENCY**

13. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction. Cryptocurrency is not illegal in the United States.

14. Bitcoin is a type of cryptocurrency. Payments or transfers of value made with bitcoins are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoins through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), Bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones.

15. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities



1 behind the public addresses are not recorded on these public ledgers. If, however, an  
2 individual or entity is linked to a public address, it may be possible to determine what  
3 transactions were conducted by that individual or entity. Bitcoin transactions are  
4 therefore sometimes described as “pseudonymous,” meaning that they are partially  
5 anonymous. And while it is not completely anonymous, Bitcoin allows users to transfer  
6 funds more anonymously than would be possible through traditional banking and credit  
7 systems.

8       16. Cryptocurrency is stored in a virtual account called a wallet. Wallets are  
9 software programs that interface with blockchains and generate and/or store public and  
10 private keys used to send and receive cryptocurrency. A public key (or public address) is  
11 akin to a bank account number, and a private key (or private address) is akin to a Personal  
12 Identification Number (“PIN”) number or password that allows a user the ability to  
13 access and transfer value associated with the public address or key. To conduct  
14 transactions on a blockchain, an individual must use the public key and the private key.  
15 A public address is represented as a case-sensitive string of letters and numbers. Each  
16 public address is controlled and/or accessed through the use of a unique corresponding  
17 private key—the cryptographic equivalent of a password or PIN—needed to access the  
18 address. Only the holder of an address’s private key can authorize any transfers of  
19 cryptocurrency from that address to another cryptocurrency address.

20       17. Although cryptocurrencies such as Bitcoin have legitimate uses,  
21 cryptocurrency is also used by individuals and organizations for criminal purposes such  
22 as money laundering, and is an oft-used means of payment for illegal goods and services  
23 on hidden services websites operating on the Tor network. By maintaining multiple  
24 wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law  
25 enforcement’s efforts to track purchases within the dark web marketplaces.

26       18. Exchangers and users of cryptocurrencies store and transact their  
27 cryptocurrency in a number of ways, as wallet software can be housed in a variety of  
28 forms, including: on a tangible, external device (“hardware wallet”); downloaded on a

1 Personal Computer (“PC”) or laptop (“desktop wallet”); with an Internet-based cloud  
2 storage provider (“online wallet”); as a mobile application on a smartphone or tablet  
3 (“mobile wallet”); as printed public and private keys (“paper wallet”); and as an online  
4 account associated with a cryptocurrency exchange. Because these desktop, mobile, and  
5 online wallets are electronic in nature, they are located on mobile devices (e.g., smart  
6 phones or tablets) or at websites that users can access via a computer, smart phone, or any  
7 device that can search the Internet. Moreover, hardware wallets are located on some type  
8 of external or removable media device, such as a Universal Serial Bus (“USB”) thumb  
9 drive or other commercially available device designed to store cryptocurrency (e.g.  
10 Trezor, Keepkey, or Nano Ledger). In addition, paper wallets may contain an address  
11 and a QR code with the public and private key embedded in the code. Paper wallet keys  
12 are not stored digitally. Wallets can also be backed up into, for example, paper printouts,  
13 USB drives, or CDs, and accessed through a “recovery seed” (random words strung  
14 together in a phrase) or a complex password. Additional security safeguards for  
15 cryptocurrency wallets can include two-factor authorization (such as a password and a  
16 phrase).

#### 17 **STATEMENT OF PROBABLE CAUSE**

18 19. In June 2019, HSI Seattle received information from the Joint Criminal  
19 Opioid and Darknet (JCODE) Team—an FBI-led task force targeting illegal opioid  
20 distribution on the dark web—regarding a dark web vendor using a certain moniker  
21 (hereinafter the “Subject Moniker”). JCODE identified the Subject Moniker as an opioids  
22 trafficker based on his trafficking activities on “Empire Market,” a dark web marketplace  
23 where, among other things, illegal drugs are frequently traded. The Subject Moniker’s  
24 profile on Empire Market indicated that he sold heroin, cocaine, and methamphetamine.  
25 The Subject Moniker also indicated that he accepted cryptocurrency in exchange for  
26 drugs, including bitcoin and Monero. There was no indication that the Subject Moniker  
27 was receiving other forms of payment.  
28

1           20.   Open source research conducted by JCODE around Empire Market and the  
2 dark web revealed the following:

3               a.     The Subject Moniker had made 32 sales on Empire Market since  
4 April 2019 with 100% positive feedback.

5               b.     The Subject Moniker's Empire Market vendor profile listed his  
6 operating hours and shipping times in Pacific Standard Time.

7               c.     At least one dark web user identified the Subject Moniker as a  
8 heroin seller who shipped from "[N]orthwest US" on a popular dark web forum in May  
9 2019.

10              d.     The same dark web forum also had postings authored by a user  
11 whose name was identical to the Subject Moniker, in which the user discussed how to  
12 pack illegal drugs, purchase postage, store drugs and packaging materials, and track  
13 shipments.

14              e.     The Subject Moniker used a messaging app called Wickr to  
15 communicate with his potential customers. The Subject Moniker's Wickr account was  
16 identical to the Subject Moniker.

17           21.   On August 20, 2019, I analyzed the PGP public key the Subject Moniker  
18 used to communicate on Empire Market. The analysis revealed that the registrant of the  
19 Subject Moniker's PGP public key listed mozzzy.phx@protonmail.com as his email  
20 address.

21           22.   On August 28, 2019, an HSI undercover agent (hereinafter "UCA") visited  
22 the Subject Moniker's store on Empire Market. The Subject Moniker was advertising  
23 "Pure #4 China White Uncut Heroin." The advertisement said: "This is 99% China White  
24 #4 Heroin straight from Sinaloa, no fentanyl or other bullshit cut here. You will not regret  
25 buying this product. It has a powdery, fluffy texture. OD's are potentially possible with  
26 opiate naïve individuals so PLEASE DO NOT ORDER THIS IF YOU CAN'T HANDLE  
27 STRONG HEROIN/OPIATES. We recommend starting with doses not greater than 5-10  
28

1 mg for total beginners.” The Subject Moniker offered 3.5 grams of “China White” heroin  
2 for \$345.00 and USPS Priority Mail shipping for \$8.

3 23. On the same day, the UCA ordered 3.5 grams of “China White” heroin  
4 from the Subject Moniker’s store on Empire Market and paid 0.03648636 Bitcoin (BTC),  
5 which was, at the time, worth approximately \$353 U.S. dollars (\$345 for heroin plus \$8  
6 for shipping). The UCA then sent the shipping instruction to the Subject Moniker through  
7 a message encrypted with Subject Moniker’s PGP public key.

8 24. On August 28, 2019, the UCA visited Empire Market again and checked  
9 the order status on the Subject Moniker’s store. The status showed that the order had been  
10 shipped via USPS Priority Mail on August 30, 2019.

11 25. On September 4, 2019, HSI Yakima received a parcel at the undercover  
12 address provided to the Subject Moniker for the “China White” heroin order. HSI  
13 Yakima forwarded the parcel to HSI Seattle via FedEx.

14 26. On September 5, 2019, HSI Seattle investigators received the parcel from  
15 HSI Yakima and opened it. The parcel contained a white envelope. Inside the white  
16 envelope was a black DVD case. The DVD case, in turn, contained multiple layers of  
17 packaging. After removing the multiple layers of packaging, the investigators recovered a  
18 zip-lock baggie with a hard rock and powdery white substance. The substance, which  
19 weighed approximately 3.94 grams with packaging, field-tested positive for heroin.

20 27. On September 6, 2019, HSI Seattle investigators visited the Subject  
21 Moniker’s store on Empire Market again. The Subject Moniker’s profile page listed the  
22 following information under the “About” section:

23 a. “9/4 – Meth is back in stock (for now, it’s going very quick so place  
24 an order ASAP if you want any), and China White is currently out of stock. China should  
25 be in stock early next week, don’t message me when it’s coming back. I’ll post here when  
26 it’s in stock.”

27 b. “9/1 – SUPER LOW prices for bulk 70% cocaine right now, not  
28 going to be in stock for long!”

1 c. “8/16 – 90% Pure Cocaine, and Social 70% Pure Cocaine have been  
2 added. The 90% is honestly the purest cocaine you will ever do hands down. It’s pricey  
3 because there’s nothing that compares to it, it’s very intense if you’re just a casual  
4 snorter. The Social Cocaine is preferred by a lot of customers because it’s very smooth  
5 and isn’t intense and still an excellent high while also being more affordable.”

6 28. An HSI analyst conducted open source research on historic dark web  
7 vendors in an attempt to identify the Subject Moniker and located information regarding  
8 Tristan BRENNAND. In 2015, HSI Seattle and U.S. Postal Inspection Service (USPIS)  
9 investigated and arrested BRENNAND for distributing MDMA on the dark web.  
10 BRENNAND was subsequently prosecuted in this District and sentenced to 48 months in  
11 prison and three years supervised release. He is currently on supervised release in this  
12 District.

13 29. Open-source research revealed that BRENNAND served his federal  
14 sentence at FCI Phoenix. In addition, a commercial database often utilized by law  
15 enforcement showed that BRENNAND was associated with 8445 N 23<sup>rd</sup> Ave, Apt 133,  
16 Phoenix, AZ 85021 between June and July 2017. Notably, the “.phx” in “mozzy.phx” is a  
17 commonly used abbreviation for Phoenix, AZ.

18 30. Independently from HSI’s research, in October 2019 the USPIS identified  
19 records related to suspicious outgoing parcels from the Bitter Lake Post Office in Seattle,  
20 WA. This record review was done as part of the USPIS’s routine inspection to detect any  
21 suspicious mailing patterns. According to the records, on September 20, 2019,  
22 approximately 57 Priority and Express Mail parcels were mailed with a listed sender of  
23 “Realtime CD and DVD Duplication.” Significantly, the parcel HSI received from the  
24 Subject Moniker on September 4, 2019 contained a DVD case with heroin inside. The  
25 listed sender for the September 4 parcel from the Subject Moniker was “Sparrow Media  
26 and Gift.”

27 31. On October 23, 2019, the USPIS, at the request of HSI Seattle, researched  
28 BRENNAND’s name on USPS databases. The USPIS discovered that BRENNAND had

1 an online U.S. Postal Service business account, and the user name for that account was  
2 “mozzy.phx.”

3 32. The USPIS recovered surveillance video footage from the Bitter Lake Post  
4 Office taken on September 20, 2019, the day that the individual dropped off  
5 approximately 57 suspicious Priority Mail parcels. The video footage showed a white  
6 male entering the Bitter Lake Post Office carrying a box full of parcels at approximately  
7 8:39 a.m. The white male removed the parcels from a box and placed some onto the retail  
8 counter and the rest into a plastic tub near a postal clerk. The physical and facial features  
9 of the white male closely resembled those of BRENNAND as depicted and described in  
10 his Washington State Department of Licensing profile. The video footage further showed  
11 the male leaving the Bitter Lake Post Office in a black BMW with blacked-out-rims and  
12 no frontal license plate.

13 33. On October 31, 2019, the USPIS researched the federal court database and  
14 saw that a piece of mail addressed to BRENNAND and relating to his supervised release  
15 was mailed to 3718 204<sup>th</sup> ST SW, APT H101, Lynnwood, WA 98036 (the “SUBJECT  
16 PREMISES”) in September 2019. This mail was delivered to and accepted at the  
17 residence.

18 34. On the same date, the USPIS conducted surveillance around the SUBJECT  
19 PREMISES. A black BMW 535 with blacked-out-rims and no frontal license plate, but  
20 with a rear Washington license plate BQA3429 (the “SUBJECT VEHICLE”) was parked  
21 in a space outside of building H and in close proximity to the hallway leading to  
22 apartment H101.

23 35. A search of the National Law Enforcement Telecommunications System  
24 (NLETS) revealed that the SUBJECT VEHICLE was registered to a Washington  
25 company called “Sundance Media Agency.” A search of the Washington State  
26 Department of Revenue database revealed that BRENNAND was listed as the governing  
27 person for the company.



1        36. On December 4, 2019, in this District, a GPS tracking warrant was issued  
2 for the SUBJECT VEHICLE for 45 days. On December 5, 2019, HSI and United States  
3 Postal Service, Office of Inspector General (USPS-OIG), installed the GPS tracker on the  
4 SUBJECT VEHICLE.

5        37. On December 15, 2019, investigators placed an undercover order for 56  
6 grams of methamphetamine from the Subject Moniker's store on Empire Market. The  
7 payment was made in bitcoin. Investigators instructed the Subject Moniker to send the  
8 narcotics to an undercover address controlled by law enforcement in Montana.

9        38. On December 17, 2019, an HSI undercover agent placed an undercover  
10 order for 56 grams of methamphetamine from the Subject Moniker on Empire Market.  
11 The payment was made in bitcoin. The undercover agent instructed the Subject Moniker  
12 to send the narcotics to an undercover address controlled by law enforcement in  
13 Washington.

14        39. On December 18, 2019, investigators from HSI, FBI, and USPIS conducted  
15 surveillance around the SUBJECT PREMISES. At approximately 11:45 a.m., I observed  
16 a white male matching the physical description of BRENNAND entering the SUBJECT  
17 VEHICLE that was parked in a parking stall near the SUBJECT PREMISES. The  
18 SUBJECT VEHICLE departed from the area and drove southbound on I-5. The agents  
19 lost visual of the SUBJECT VEHICLE, but was later able to locate the SUBJECT  
20 VEHICLE parked near an office space located at 1455 NW Leary Way, Suite 400 (Office  
21 409), Seattle, WA 98107 (the "SUBJECT OFFICE") based on information from the GPS  
22 tracker.

23        40. At approximately 4:39 p.m., one of the investigators observed the same  
24 white male matching the physical description of BRENNAND exit from the building in  
25 which the SUBJECT OFFICE was located. The male was carrying white envelopes that  
26 were consistent in appearance with the U.S. Priority Mail parcel received by the HSI  
27 Yakima on September 4, 2019, and the U.S. Priority Mail parcels that had been dropped  
28 off at the Bitter Lake Post Office on September 20, 2019. The male placed the white

1 | envelopes in the trunk of the SUBEJCT VEHICLE, smoked or vaped near the vehicle, and  
2 | subsequently departed at approximately 4:47 p.m. Investigators followed the SUBJECT  
3 | VEHICLE but lost visual.

4 |         41.     HSI subsequently obtained records from Regus, a company that managed  
5 | the building in which the SUBJECT OFFICE was located, on January 3, 2020. The  
6 | records showed that BRENNAND had been occupying the SUBJECT OFFICE since July  
7 | 2019 under the company name T. BRENNAND, Inc. The Office Agreement was signed  
8 | by BRENNAND on July 12, 2019.

9 |         42.     On December 19, 2019, investigators placed an undercover purchase for a  
10 | half ounce of methamphetamine from the Subject Moniker's store on Empire Market.  
11 | The payment was made in bitcoin. Investigators instructed the Subject Moniker to send  
12 | the methamphetamine to an undercover address controlled by law enforcement in  
13 | Pennsylvania.

14 |         43.     On December 20, 2019, investigators from HSI, FBI, and USPIS conducted  
15 | surveillance near the SUBJECT PREMISES. At approximately 8:47 a.m., I observed a  
16 | white male matching the physical description of BRENNAND walking to the SUBJECT  
17 | VEHICLE, which was parked near the intersection of 38<sup>th</sup> Ave W and 204<sup>th</sup> St SW, with  
18 | a purple backpack and subsequently departing from the area.

19 |         44.     Investigators followed the SUBJECT VEHICLE to an office building in the  
20 | Lake City area of Seattle, WA, which appeared to be some sort of community clinic.  
21 | After staying in the area over an hour, the white male matching the physical description  
22 | of BRENNAND left the office building at approximately 12:46 p.m. Investigators who  
23 | were following the SUBJECT VEHICLE lost the track of the vehicle, but eventually re-  
24 | located it outside the SUBJECT OFFICE.

25 |         45.     Later on the same day, at approximately 5:43 p.m., an investigator observed  
26 | the same white male matching BRENNAND's physical description exit the building in  
27 | which the SUBJECT OFFICE was located and enter the SUBJECT VEHICLE.  
28 |

1 Investigators followed the SUBJECT VEHICLE from the SUBJECT OFFICE directly to  
2 the Ballard Post Office located at 5706 17<sup>th</sup> AVE NW, Seattle, WA 98107.

3 46. The investigator observed the while male parking the SUBJECT VEHICLE  
4 near the post office and exiting the car. The investigator then observed the male entering  
5 the post office and handing several parcels to an undercover USPS-OIG agent who was  
6 posing as a regular USPS employee.

7 47. Specifically, the white male handed the undercover agent five parcels with  
8 pre-printed USPS shipping labels from a third-party postage vendor. One of the parcels  
9 listed the recipient name and address provided by investigators to the Subject Moniker  
10 for the December 19, 2019 undercover purchase of methamphetamine on Empire Market.  
11 The parcel had a return address of "Mustard and Co, 6123 S Pilgrim St, Seattle, WA  
12 98188-5857."

13 48. On December 23, 2019, investigators opened the parcel associated with the  
14 December 19, 2019 undercover purchase. Inside the parcel was a manila envelope with a  
15 black DVD case inside. Inside the DVD case was a dark Mylar bag which was sealed.  
16 Inside the Mylar bag was a clear sealed bag. Inside the clear sealed bag was a plastic  
17 baggie containing a crystalline substance. The plastic baggie containing a crystalline  
18 substance weighed approximately 16.3 grams. The substance was field-tested positive  
19 for methamphetamine.

20 49. On December 27, 2019, the USPIS Seattle received the parcel associated  
21 with the December 15, 2019 undercover purchase. This parcel had been received at the  
22 undercover address in Montana that had been provided to the Subject Moniker at the time  
23 of the undercover purchase and forwarded to the USPIS Seattle by the USPIS counterpart  
24 in Montana. The parcel displayed tracking number 9405 5368 9784 6227 7369 73 with  
25 return address "ARC Document Solutions, 5211 Kensington P1 N, Seattle, WA 98103-  
26 6225."

27 50. On the same day, investigators opened the parcel. Inside the parcel was a  
28 manila envelope. Inside the manila envelope was a dark Mylar bag which was sealed.

1 Inside the Mylar bag was a clear sealed bag. Inside the clear sealed bag was a plastic  
2 baggie containing a crystalline substance. The plastic baggie containing a crystalline  
3 substance weighed approximately 58.3 grams. The substance was field-tested positive for  
4 the presence of methamphetamine.

5 51. USPS records revealed that the parcel had been first scanned at the Ballard  
6 Post Office located in Seattle on December 18, 2019 at approximately 6:33 p.m. This is  
7 the same day on which BRENNAND was seen carrying the white envelopes and placed  
8 them inside of the trunk of the SUBJECT VEHICLE parked just outside the SUBJECT  
9 OFFICE.

10 52. On January 6, 2020, HSI Yakima received the parcel associated with the  
11 December 17, 2019 undercover purchase at the undercover address provided to the  
12 Subject Moniker. HSI Yakima subsequently forwarded the parcel to HSI Seattle. The  
13 parcel displayed USPS tracking number 9405 5368 9784 6231 6145 26 with return  
14 address "ARC Document Solutions, 5211 Kensington PL N, Seattle, WA 98103-6225."

15 53. On January 7, 2020, investigators opened the parcel. Inside the parcel was a  
16 manila envelope. Inside the manila envelope was a black DVD case with two blue strips  
17 of tape holding the DVD case closed. Inside the DVD case was a black sealed Mylar bag.  
18 Inside the Mylar bag was a clear sealed bag. Inside the clear sealed bag was a clear  
19 plastic zip lock bag that contained a crystalline substance. The substance was field tested  
20 positive for methamphetamine. The plastic zip lock bag containing a crystalline substance  
21 weighed approximately 58.06 grams.

22 54. On January 14, 2020, I applied for and obtained a federal search warrant to  
23 search the SUBJECT PREMISES, SUBJECT OFFICE, SUBJECT VEHICLE, and the  
24 person of BRENNAND. On January 16, 2020, investigators executed the search warrant  
25 at, among other places, the SUBJECT OFFICE. Investigators encountered BRENNAND  
26 and a white male later identified as Maxwell GUNTER inside the SUBEJCT OFFICE. I  
27 saw BRENNAND sitting in front of two computer monitors and GUNTER standing next  
28 to BRENNAND wearing black latex gloves and with a clear view of both monitors.

1 Based on my training and experience, I know that drug traffickers who handle potent  
2 opiates—fentanyl in particular—often wear latex gloves such as the ones GUNTER was  
3 wearing to protect themselves from cutaneous absorption of such substances.  
4 BRENNAND and GUNTER were looking at the monitors when investigators opened the  
5 office door.

6 55. The right monitor was displaying a screen for Empire Market. The screen  
7 showed that BRENNAND was logged in on Empire Market as the SUBJECT  
8 MONIKER. The screen also showed that the SUBJECT MONIKER had approximately  
9 46 pending orders, some of which were for controlled substances, to be processed and  
10 that the SUBJECT MONIKER's account had a balance of 0.40611 Bitcoin (BTC) and  
11 0.00498 Litecoin (LTC). The monitor displayed three additional tabs at the top.

12 56. The left monitor was logged into Proton email account  
13 2ndchance.restoration@protonmail.com. The monitor also showed that BRENNAND  
14 was logged into mozzzy.phx@protonmail.com on a different tab. Investigators observed a  
15 PGP program running on the monitor. The monitor displayed several additional tabs at  
16 the top.

17 57. Investigators searching the SUBJECT OFFICE subsequently located a  
18 cabinet drawer containing several large bags with a white powdery substance inside. The  
19 bags had the writing "No label Fent 1 sticker," "2 sticker fent," "Cali" and "China Pony"  
20 on them. Based on my training and experience the term "fent" is an abbreviated term  
21 often used by drug dealers for fentanyl. All the white powders had a combined weight of  
22 approximately 3.64 kilograms with packaging.

23 58. In addition to the white powders, agents found the following items in the  
24 same cabinet:

25 a. A bag of an off-white substance that field-tested positive for cocaine  
26 and weighed approximately 211 grams with packaging;

27 b. A bag of an off-white substance that field-tested positive for cocaine  
28 and weighed approximately 1.37 kilograms with packaging;

1 c. A bag containing a black tar-like substance that tested presumptively  
2 positive for heroin using a MX908 Hand Held Mass Spectrometer and weighed  
3 approximately 290 grams with packaging;

4 d. A sample of white powder contained in a plastic bag with "23.79"  
5 written on the bag that tested presumptively positive for the presence of fentanyl using a  
6 MX908 Hand Held Mass Spectrometer; and

7 e. Multiple green pills that resembled Xanax bars but were colored  
8 green; based on my training and experience, I know that these pills are known as "Hulks"  
9 due to their color. The combined weight of the pills were approximately 2.40 kilograms.  
10 Agents later tested white powder residues that were left outside the bag containing these  
11 pills using the MX908 device. The residues tested presumptively positive for the  
12 presence of fentanyl.

13 59. In the trunk of BRENNAND's BMW, investigators found a parcel  
14 addressed to "Austin Burgess" at 2442 Northwest Market Street, Seattle, WA. A US  
15 Postal Inspector subsequently went to 2442 Northwest Market Street, Seattle, WA, which  
16 was the address for Ballard Mailbox and Shipping Center. An employee advised a parcel  
17 addressed to "Austin Burgess" was being held at will call for pickup. On January 21,  
18 2020, an HSI agent obtained the parcel from Ballard Mailbox and Shipping Center. On  
19 January 30, 2020, a federal postal warrant was executed on the parcel. Discovered inside  
20 the parcel were approximately 1,132.4 grams of methamphetamine and approximately  
21 82.1 grams of heroin, field-tested positive as such.

22 60. In addition, during the search that took place on January 16, 2020,  
23 investigators found from BRENNAND's wallet a fictitious California driver license  
24 bearing BRENNAND's picture and the name "Austin Burgess." This fictitious license  
25 was located behind BRENNAND's Washington State driver's license. Investigators also  
26 found a copy of the lease agreement at Active Space, a storage company, in the name of  
27 "Austin Burgess" from the SUBJECT OFFICE. I later obtained records from Active  
28 Space regarding a storage unit for "Austin Burgess." The records obtained from Active



1 Space included the rental application for the **SUBJECT STORAGE UNIT** in the name  
2 of “Austin Burgess” and a photocopy of the same fictitious CA driver license found in  
3 BRENNAND’s wallet. The lease agreement listed Austin.Burgess@protonmail.com and  
4 Sundance Media LLC as Austin Burgess’s email address and employer.

5 61. A review of U.S Customs and Border Protection (CBP) import records  
6 associated with “Austin Burgess” revealed that multiple import parcels had been shipped  
7 to “Austin Burgess” at the **SUBJECT STORAGE UNIT** between November and  
8 December of 2019. Three of those parcels were shipped from South Korea and declared  
9 as “packaging machine accessories iron” with declared weights between 128 and 150  
10 pounds. One such parcel was shipped from China and declared as “mixing machine iron  
11 home use” with a declared weight of 101 kg. The parcel from China was inspected by the  
12 U.S. Customs and Border Protection but was released after no contraband was found.  
13 Another parcel was shipped from Hong Kong and declared as “accessories” with a  
14 declared weight of 5 kg.

15 62. Based on my training and experience, and the description and declared  
16 weight of the items shipped, I suspect that the imported items were potentially used to  
17 facilitate BRENNAND’s drug trafficking activities such as packaging and manufacturing  
18 of controlled substances at the **SUBJECT STORAGE UNIT**.<sup>2</sup>

19 **TACTICS USED BY DRUG TRAFFICKERS**

20 63. Based upon my training and experience, and conversations with other  
21 experienced law enforcement agents and officers who have been involved in narcotics  
22 cases, I know the following.

23 64. The distribution of illegal narcotics is frequently a continuing activity  
24 lasting over months and years. Persons involved in the trafficking of illegal controlled  
25

26 \_\_\_\_\_  
27 <sup>2</sup> It should be noted that on January 17, 2020, a Canine Officer with U.S. Customs and Border Protection and K-9  
28 REMI sniffed a row of storage units at 4020 Leary Way NW, Seattle, WA, including the **SUBJECT STORAGE**  
UNIT. K-9 REMI alerted to storage unit #127 for the presence of controlled substances. K-9 REMI did not alert to  
storage unit #129 for the presence of controlled substances.

1 substances typically will obtain and distribute controlled substances on a regular basis,  
2 much as a distributor of a legal commodity would purchase stock for sale. Similarly, such  
3 drug traffickers will maintain an “inventory” which will fluctuate in size depending upon  
4 the demand for and the available supply of the product. Drug traffickers often keep  
5 records of their illegal activities not only during the period of their drug trafficking  
6 violations but also for a period of time extending beyond the time during which the  
7 trafficker actually possesses/controls illegal controlled substances. The records are kept  
8 in order to maintain contact with criminal associates for future transactions and so that  
9 the trafficker can have records of prior transactions for which the trafficker might still be  
10 owed money or might owe someone else money. Drug traffickers often keep these  
11 records in their homes and in vehicles that they own, use, or have access to.

12 65. It is common for drug traffickers to conceal large quantities of U.S.  
13 currency, foreign currency, cryptocurrency, financial instruments, precious metals,  
14 jewelry, and other items of value which are proceeds from drug trafficking in their  
15 residences and in other storage areas associated with the residence, such as on-site  
16 storage lockers, garages, detached storage sheds, and parking stalls, or safes located on  
17 the property.

18 66. Evidence of excessive wealth beyond an individual’s outward means is  
19 probative evidence of the distribution of controlled substances. Therefore, receipts  
20 showing the expenditure of large sums of money and/or the expensive assets can be  
21 evidence of drug trafficking. Drug traffickers commonly keep the expensive assets  
22 themselves and/or documentation of the purchase of the asset (receipts, warranty cards,  
23 etc.) in their homes, places of business, and in vehicles that they own, use, or have access  
24 to.

25 67. It is common for drug traffickers to maintain equipment and supplies (*i.e.*,  
26 scales, packaging, masking agents) on hand over a lengthy period of time, even when  
27 they do not have any controlled substances on hand. The aforementioned items are  
28

1 frequently maintained in the drug trafficker's homes, places of business, stash houses, or  
2 storage units, and in vehicles that they own, use, or have access to.

3 68. Drug traffickers often have some amount of inventory—namely, illegal  
4 drugs—stored in their homes, places of business, stash houses or storage units, and in  
5 vehicles that they own, use, or have access to.

6 69. It is common for drug traffickers to possess firearms and ammunition to  
7 protect their drugs, assets, and persons from hostile gangs, rival traffickers, other  
8 criminals, and from law enforcement. Persons who purchase and possess firearms also  
9 tend to maintain the firearms and ammunition for lengthy periods of time. Firearms can  
10 be acquired both legally and unlawfully, without official/traceable documentation.  
11 Persons who acquire firearms from Federal Firearms Licensees, through deliberate fraud  
12 and concealment, often will also acquire firearms from private parties and other sources  
13 unknown to the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”). Persons  
14 who, whether legally or illegally, purchase, possess, sell and/or transfer firearms or  
15 ammunition commonly maintain the firearms or ammunition on their person, at their  
16 residence or business, or in a motor vehicle which they own and/or operate. Firearms or  
17 ammunition are often secreted at other locations within their residential curtilage, and the  
18 identification of these firearms will assist in establishing their origin. Persons who  
19 purchase, possess, sell and/or trade firearms or ammunition commonly maintain  
20 documents and items that are related to the purchase, ownership, possession, sale and/or  
21 transfer of firearms, ammunition, and/or firearm parts, including but not limited to  
22 driver's licenses, telephone records, telephone bills, address and telephone books,  
23 canceled checks, receipts, bank records and other financial documentation on the owner's  
24 person, at the owner's residence or business, or in vehicles that they own, use, or have  
25 access to. Additionally, these individuals often maintain holsters, spare magazines or  
26 speed loaders and other instruments to facilitate the use of firearms in furtherance of  
27 criminal activity or acts of violence.  
28

1       70. It is common for members of drug trafficking organizations, in an attempt  
2 to disguise their identities and illegal activities, to use prepaid cellular telephones and  
3 prepaid long-distance calling cards. Often the only way to connect a subject with a  
4 particular prepaid cellular telephone or calling card is to seize the phone or calling card  
5 from the trafficker or his residence. The aforementioned items are frequently maintained  
6 in the drug trafficker's residence, place of business, or other areas they have access to.

7       71. Drug traffickers often carry many of the items described above—including  
8 (but not limited to) drugs, drug proceeds, firearms, cellular phones—on their person.

9       72. Drug dealers regularly use cell phones and other electronic communication  
10 devices to further their illegal activities. As a result, evidence of drug dealing can often  
11 be found in text messages, address books, call logs, photographs, emails, text messaging  
12 or picture messaging applications, videos, and other data that is stored on cell phones and  
13 other electronic communication devices. Additionally, the storage capacity of such  
14 devices allows them to be used for the electronic maintenance of ledgers, pay/owe logs,  
15 drug weights and amounts, customers contact information, not only during the period of  
16 their drug trafficking violations but also for a period of time extending beyond the time  
17 during which the trafficker actually possesses/controls illegal controlled substances. The  
18 records are kept in order to maintain contact with criminal associates for future  
19 transactions and so that the trafficker can have records of prior transactions for which the  
20 trafficker might still be owed money or might owe someone else money.

21       73. Drug traffickers increasingly use applications on smartphones that encrypt  
22 communications such as WhatsApp, or applications that automatically delete messages,  
23 such as Snapchat, in order to avoid law enforcement monitoring or recording of  
24 communications regarding drug trafficking and/or money laundering. Evidence of the  
25 use of such applications can be obtained from smartphones and is evidence of a  
26 smartphone user's efforts to avoid law enforcement detection.

27       **USE OF DIGITAL DEVICES AND DARK WEB SALES**  
28

1        74. As a result of my training and experience, I know that digital devices must  
2 be used by individuals who engage in dark web drug sales. Suspects engaged in dark  
3 web drug sales use digital devices, such as computers and smartphones, and often  
4 transport those digital devices while conducting illegal activity. In particular, a suspect  
5 needs digital device equipped with Tor software to access the Internet in order to navigate  
6 the dark web marketplaces referenced in this affidavit. Digital devices are further needed  
7 to establish a dark web persona; list contraband for sale; communicate with customers  
8 and associates on a dark web marketplace, through encrypted messages and other means;  
9 and to transfer digital currency from a marketplace to another wallet. As a result, one  
10 form in which these items may be found is as electronic evidence stored on a digital  
11 device.

12        75. I know that Tor software exists for both computers and smartphones that  
13 allow a user to access the dark web. For example, Tor Browser is freely available for  
14 download and allows for the use of Tor on computers. Tor Browser can also be run off a  
15 USB flash drive once inserted into a computer. In addition, Tor is available for Android  
16 phones by installing the package named Orbot. Orbot brings the features and  
17 functionality of Tor to the Android mobile operating system.

18        76. While Tor is designed to protect a user's anonymity and privacy on the  
19 Internet, some artifacts may be recovered by a computer forensic examiner. Artifacts  
20 which may be found on a digital device equipped with Tor include the mere existence of  
21 a Tor application, as well as websites bookmarked by a user. While the installation of  
22 Tor in and of itself is not nefarious, the existence of the application would show a user  
23 had the ability to access the dark web. Furthermore, bookmarked websites would show  
24 sites a user visited.

25        77. Furthermore, I know that PGP applications exist for both computers and  
26 smartphones. PGP is often used to encrypt communication between individuals who  
27 operate on dark web markets. Forensic examination of digital devices may reveal the  
28

1 existence of PGP applications and keys. Extracted PGP keys may help investigators link  
2 a digital device and/or a suspect to a dark web identity.

3 78. As the case with most digital technology, communications by way of  
4 computer can be saved or stored on the computer used for these purposes. Storing this  
5 information can be intentional, *i.e.*, by saving an e-mail as a file on the computer or  
6 saving the location of one's favorite websites in, for example, "bookmark" files. Digital  
7 information can also be retained unintentionally. For example, traces of the path  
8 (including, but not limited to, the IP address) of an electronic communication may be  
9 automatically stored in many places (e.g., temporary files or ISP client software, among  
10 others). In addition to electronic communications, a computer user's Internet activities  
11 generally leave traces or "footprints" in the web cache and history files of the browser  
12 used. In other words, if a computer user were to go to the website called  
13 WWW.USDOJ.GOV, a "footprint" in the browser cache may be found pointing to that  
14 website, indicating that particular computer was used to visit that website. Therefore, a  
15 search of digital devices may lead to evidence that will assist me in identifying online  
16 storage accounts for which I may be able to obtain additional search warrants to locate  
17 further evidence in this case.

18 79. In addition, I know, based on my training and experience, that those  
19 engaged in dark web drug sales use digital devices to, for example: a) store PGP keys; b)  
20 store customer shipping information; c) store cryptocurrency wallets; d) store  
21 photographs of narcotics; and e) purchase and print postage/shipping labels.

22 80. In my experience, dark web drug vendors often use digital devices such as  
23 smartphones to take photographs of drugs. Vendors then transfer the photographs to a  
24 computer, which is used to list their drugs for sale on a dark web marketplace.  
25 Furthermore, dark web drug vendors often use computers to type and print postage labels  
26 which are attached to parcels containing drugs shipped to customers. This is because  
27 typing both the sender and recipient information for labels on a smartphone is a tedious  
28 task, which is much easier using a computer with a keyboard.



**SEARCH AND SEIZURE OF DIGITAL MEDIA**

81. As described above and in Attachment B, this application seeks permission to search for items listed in Attachment B that might be found in the **SUBJECT STORAGE UNIT**.

82. In order to examine digital media in a forensically sound manner, law enforcement personnel, with appropriate expertise, will conduct a forensic review of any digital media seized. The purpose of using specially trained computer forensic examiners to conduct the imaging of any digital media or digital devices is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners and investigators often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, may lack the factual and investigative expertise that an investigate agent may possess. Therefore, computer forensic examiners and agents often work closely together. It is intended that the warrant will provide authority for the affiant to forensically review, or seek the assistance of others in the HSI or within other law enforcement agencies to assist in the forensic review of any digital devices.

83. I also know the following:

a. Based my knowledge, training, and experience, I know that computer files or remnants of such files may be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, this information can sometimes be recovered months or years later with forensics tools. This is because when a person "deletes" a file on a computer, the data contained in the files does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

1           b.       Therefore, deleted files, or remnants of deleted files, may reside in  
2 free space or slack space—that is, in space on the storage medium that is not currently  
3 being used by an active file—for long periods of time before they are overwritten. In  
4 addition, a computer’s operating system may also keep a record of deleted data in “swap”  
5 or “recovery” files.

6           c.       Wholly apart from user-generated files, computer storage media—in  
7 particular, computers’ internal hard drives—contain electronic evidence of how a  
8 computer has been used, what it has been used for, and who has used it. To give a few  
9 examples, this forensic evidence can take the form of operating system configurations,  
10 artifacts from operating system or application operation, file system data structures, and  
11 virtual memory “swap” paging files. Computer users typically do not erase or delete this  
12 evidence, because special software is typically required for that task. However, it is  
13 technically possible to delete this information.

14           d.       Similarly, files that have been viewed via the Internet are sometimes  
15 automatically downloaded into a temporary Internet directory or “cache.”

16           e.       Digital storage devices may also be large in capacity, but small in  
17 physical size. Those who are in possession of such devices also tend to keep them on  
18 their persons, especially when they may contain evidence of a crime. Digital storage  
19 devices may be smaller than a postal stamp in size, and thus they may easily be hidden in  
20 a person’s pocket.

21       84.       As further described in Attachment B, this application seeks permission to  
22 locate not only computer files that might serve as direct evidence of the crimes described  
23 on the warrant, but also for forensic electronic evidence that establishes how computers  
24 were used, the purpose of their use, who used them, and when. There is probable cause to  
25 believe that this forensic electronic evidence will be on digital devices found in the

26 **SUBJECT STORAGE UNIT:**

27           a.       Data on the digital storage medium or digital devices can provide  
28 evidence of a file that was once on the digital storage medium or digital devices but has

1 since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has  
2 been deleted from a word processing file). Virtual memory paging systems can leave  
3 traces of information on the storage medium that show what tasks and processes were  
4 recently active. Web browsers, e-mail programs, and chat programs store configuration  
5 information on the storage medium that can reveal information such as online nicknames  
6 and passwords. Operating systems can record additional information, such as the  
7 attachment of peripherals, the attachment of USB flash storage devices or other external  
8 storage media, and the times the computer was in use. Computer file systems can record  
9 information about the dates files were created and the sequence in which they were  
10 created, although this information can later be falsified.

11           b. As explained herein, information stored within a computer and other  
12 electronic storage media may provide crucial evidence of the “who, what, why, when,  
13 where, and how” of the criminal conduct under investigation, thus enabling the United  
14 States to further establish and prove each element or alternatively, to exclude the innocent  
15 from further suspicion. In my training and experience, information stored within a  
16 computer or storage media (*e.g.*, registry information, communications, images and  
17 movies, transactional information, records of session times and durations, Internet  
18 history, and anti-virus, spyware, and malware detection programs) can indicate who has  
19 used or controlled the computer or storage media. This “user attribution” evidence is  
20 analogous to the search of “indicia of occupancy” while executing a search warrant at a  
21 residence. The existence or absence of anti-virus, spyware, and malware detection  
22 programs may indicate whether the computer was remotely accessed, thus inculcating or  
23 exculpating the computer owner. Further computer and storage media activity can  
24 indicate how and when the computer or storage media was accessed or used. For  
25 example, as described herein, computers typically contain information that log computer  
26 activity associated with user accounts and electronic storage media connected with the  
27 computer. Such information allows investigators to understand the chronological context  
28 of computer or electronic storage media access, use, and events relating to the crime

1 under investigation. Additionally, some information stored within a computer or  
2 electronic storage media may provide crucial evidence relating to the physical location of  
3 other evidence and the suspect. For example, images stored on a computer may both  
4 show a particular location and have geolocation information incorporated into its file  
5 data. Such file data typically also contains information indicating when the file or image  
6 was created. The existence of such image files, along with external device connection  
7 logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital  
8 camera or cellular phone with an incorporated camera). The geographic and timeline  
9 information described herein may either inculcate or exculpate the computer user.  
10 Lastly, information stored within a computer may provide relevant insight into the  
11 computer user's state of mind as it relates to the offense under investigation. For  
12 example, information within the computer may indicate the owner's motive and intent to  
13 commit the crime (*e.g.*, Internet searches indicating criminal planning), or consciousness  
14 of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or  
15 password protecting/encrypting such evidence in an effort to conceal it from law  
16 enforcement).

17 c. A person with appropriate familiarity with how a computer works  
18 can, after examining this forensic evidence in its proper content, draw conclusions about  
19 how computers were used, the purpose of their use, who used them, and when.

20 d. The process of identifying the exact files, blocks, registry entries,  
21 logs, or other forms of forensic evidence on a storage medium that are necessary to draw  
22 an accurate conclusion is a dynamic process. While it is possible to specify in advance  
23 the records to be sought, computer evidence is not always data that can be merely  
24 reviewed by a review team and passed along to investigators. Whether data stored on a  
25 computer is evidence may depend on other information stored on the computer and the  
26 application of knowledge about how a computer behaves. Therefore, contextual  
27 information necessary to understand other evidence also falls within the scope of the  
28 warrant.

1 e. Further, in finding evidence of how a computer was used, the  
2 purpose of its use, who used it, and when, sometimes it is necessary to establish that a  
3 particular thing is not present on a storage medium. For example, the presence or  
4 absence of counter-forensic programs or anti-virus programs (and associated data) may  
5 be relevant to establishing a user's intent.

6 85. In most cases, a thorough search of a premises for information that might  
7 be stored on digital storage media or other digital devices often requires the seizure of the  
8 digital devices and digital storage media for later off-site review consistent with the  
9 warrant. In lieu of removing storage media from the premises, it is sometimes possible to  
10 make an image copy of storage media. Generally speaking, imaging is the taking of a  
11 complete electronic copy of the digital media's data, including all hidden sectors and  
12 deleted files. Either seizure or imaging is often necessary to ensure the accuracy and  
13 completeness of data recorded on the storage media, and to prevent the loss of the data  
14 either from accidental or intentional destruction. This is true because of the following:

15 a. *The time required for an examination.* As noted above, not all  
16 evidence takes the form of documents and files that can be easily viewed on site.  
17 Analyzing evidence of how a computer has been used, what it has been used for, and who  
18 has used it requires considerable time, and taking that much time on premises could be  
19 unreasonable. As explained above, because the warrant calls for forensic electronic  
20 evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage  
21 media to obtain evidence. Storage media can store a large volume of information.  
22 Reviewing that information for things described in the warrant can take weeks or months,  
23 depending on the volume of data stored, and would be impractical and invasive to  
24 attempt on-site.

25 b. *Technical requirements.* Computers can be configured in several  
26 different ways, featuring a variety of different operating systems, application software,  
27 and configurations. Therefore, searching them sometimes requires tools or knowledge  
28 that might not be present on the search site. The vast array of computer hardware and

1 software available makes it difficult to know before a search what tools or knowledge  
2 will be required to analyze the system and its data on-site. However, taking the storage  
3 media off-site and reviewing it in a controlled environment will allow its examination  
4 with the proper tools and knowledge.

5 c. *Variety of forms of electronic media.* Records sought under this  
6 warrant could be stored in a variety of storage media formats that may require off-site  
7 reviewing with specialized forensic tools.

8 86. Searching computer systems is a highly technical process that requires  
9 specific expertise and specialized equipment. There are so many types of computer  
10 hardware and software in use today that it is rarely possible to bring to the search site all  
11 the necessary technical manuals and specialized equipment necessary to consult with  
12 computer personnel who have expertise in the type of computer, operating system, or  
13 software application being searched.

14 87. The analysis of computer systems and storage media often relies on  
15 rigorous procedures designed to maintain the integrity of the evidence and to recover  
16 “hidden,” mislabeled, deceptively named, erased, compressed, encrypted or password-  
17 protected data, while reducing the likelihood of inadvertent or intentional loss or  
18 modification of data. A controlled environment such as a laboratory, is typically required  
19 to conduct such an analysis properly.

20 88. The volume of data stored on many computer systems and storage devices  
21 will typically be so large that it will be highly impracticable to search for data during the  
22 execution of the physical search of the premises. The hard drives commonly included in  
23 desktop and laptop computers are capable of storing millions of pages of text.

24 89. A search of digital devices for evidence described in Attachment B may  
25 require a range of data analysis techniques. In some cases, agents may recover evidence  
26 with carefully targeted searches to locate evidence without requirement of a manual  
27 search through unrelated materials that may be commingled with criminal evidence.

28 Agents may be able to execute a “keyword” search that searches through the files stored

1 in a digital device for special terms that appear only in the materials covered by the  
2 warrant. Or, agents may be able to locate the materials covered by looking for a  
3 particular directory or name. However, in other cases, such techniques may not yield the  
4 evidence described in the warrant. Individuals may mislabel or hide files and directories;  
5 encode communications to avoid using keywords; attempt to delete files to evade  
6 detection; or take other steps designed to hide information from law enforcement  
7 searches for information.

8 90. The search procedure of any digital device seized may include the  
9 following on-site techniques to seize the evidence authorized in Attachment B:

10 a. On-site triage of computer systems to determine what, if any,  
11 peripheral devices or digital storage units have been connected to such computer systems,  
12 a preliminary scan of images files contained on such systems and digital storage devices  
13 to help identify any other relevant evidence or co-conspirators.

14 b. On-site copying and analysis of volatile memory, which is usually  
15 lost if a computer is powered down and may contain information about how the computer  
16 is being used, by whom, when and may contain information about encryption, virtual  
17 machines, or stenography which will be lost if the computer is powered down.

18 c. On-site forensic imaging of any computers may be necessary for  
19 computers or devices that may be partially or fully encrypted in order to preserve  
20 unencrypted data that may, if not immediately imaged on-scene become encrypted and  
21 accordingly become unavailable for any examination.

22 //

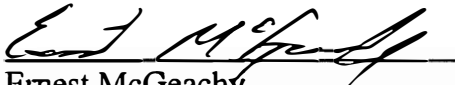
23 //

24 //



CONCLUSION

91. Based on the information set forth herein, there is probable cause to search the **SUBJECT STORAGE UNIT**, as further described in Attachment A, for evidence, fruits, and instrumentalities, as further described in Attachment B, of crimes committed by BRENNAND and his coconspirator(s), specifically distribution of, and possession of, with intent to distribute, controlled substances, in violation of Title 21, United States Code, Section 841(a)(1).

  
Ernest McGeachy  
Special Agent  
Department of Homeland Security  
Homeland Security Investigations

SWORN TO BEFORE ME PURSUANT TO CRIM. RULE 4.1 on this  
12<sup>th</sup> day of March 2020.

  
HON. MICHELLE L. PETERSON  
United States Magistrate Judge

**ATTACHMENT A**

**Place to Be Searched**

The place to be searched is 4020 Leary Way NW, Unit 129, Seattle, WA 98107 (the “**SUBJECT STORAGE UNIT**”), a single storage unit located first floor of the building. The storage unit has a gray door with a front window.



**ATTACHMENT B**

**List of Items to be Seized**

Evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Distribution of and Possession of, with Intent to Distribute, Controlled Substances), committed by Tristan BRENNAND and his co-conspirator(s), as follows:

1. Controlled Substances: Including but not limited to heroin, methamphetamine, and cocaine;

2. Drug Paraphernalia: Items used, or to be used, to store, process, package, use, and/or distribute controlled substances, such as plastic bags, DVD cases, cutting agents, scales, measuring equipment, vials, pill presses, Mylar bags, heat/vacuum sealers, tape, duffel bags, chemicals or items used to test the purity and/or quality of controlled substances, and similar items;

3. Drug Transaction Records: Documents such as ledgers, receipts, notes, and similar items relating to the acquisition, transportation, and distribution of controlled substances;

4. Customer and Supplier Information: Items identifying drug customers and drug suppliers, such as telephone records, personal address books, correspondence, diaries, calendars, notes with phone numbers and names, "pay/owe" sheets with drug amounts and prices, maps or directions, and similar items;

5. Cash and Financial Records: Currency and financial records, including bank records, safe deposit box records and keys, credit card records, bills, receipts, tax returns, vehicle documents, and similar items; and other records that show income and expenditures, net worth, money transfers, wire transmittals, negotiable instruments, bank drafts, cashier's checks, and similar items, and money counters;

6. Photographs/Surveillance: Photographs, video tapes, digital cameras, surveillance cameras and associated hardware/storage devices, and similar items, depicting property occupants, friends and relatives of the property occupants, or suspected buyers or sellers of controlled substances, controlled substances or other contraband, weapons, and assets derived from the distribution of controlled substances;

7. Weapons: Including firearms, magazines, ammunition, and body armor;

1        8.        Codes: Evidence of codes used in the distribution of controlled substances,  
2 including passwords, code books, cypher or decryption keys, usernames and/or  
3 credentials for dark web marketplaces, and similar information;

4        9.        Property Records: Deeds, contracts, escrow documents, mortgage  
5 documents, rental documents, and other evidence relating to the purchase, ownership,  
6 rental, income, expenses, or control of the premises, and similar records of other property  
7 owned or rented;

8        10.       Indicia of occupancy, residency, and/or ownership of assets including,  
9 utility and telephone bills, canceled envelopes, rental records or payment receipts, leases,  
10 mortgage statements, and other documents;

11       11.       Evidence of Storage Unit Rental or Access: Rental and payment records,  
12 keys and codes, pamphlets, contracts, contact information, directions, passwords or other  
13 documents relating to storage units;

14       12.       Evidence of Personal Property Ownership: Registration information,  
15 ownership documents, or other evidence of ownership of property including, but not  
16 limited to vehicles, vessels, boats, airplanes, jet skis, all-terrain vehicles, RVs, and  
17 personal property; evidence of international or domestic travel, hotel/motel stays, and any  
18 other evidence of unexplained wealth;

19       13.       Individual and business financial books, records, receipts, notes, ledgers,  
20 diaries, journals, and all records relating to income, profit, expenditures, or losses, such  
21 as:

22           b.       Employment records: paychecks or stubs, lists and accounts of  
23 employee payrolls, records of employment tax withholdings and  
24 contributions, dividends, stock certificates, and compensation to  
25 officers.

26           c.       Savings accounts: statements, ledger cards, deposit tickets, register  
27 records, wire transfer records, correspondence, and withdrawal slips.

28           d.       Checking accounts: statements, canceled checks, deposit tickets,  
credit/debit documents, wire transfer documents, correspondence, and  
register records.

          e.       Loan Accounts: financial statements and loan applications for all loans  
applied for, notes, loan repayment records, and mortgage loan records.

          f.       Collection accounts: statements and other records.

- g. Certificates of deposit: applications, purchase documents, and statements of accounts.
- h. Credit card accounts: credit cards, monthly statements, and receipts of use.
- i. Receipts and records related to gambling wins and losses, or any other contest winnings.
- j. Insurance: policies, statements, bills, and claim-related documents.
- k. Financial records: profit and loss statements, financial statements, receipts, balance sheets, accounting work papers, any receipts showing purchases made, both business and personal, receipts showing charitable contributions, and income and expense ledgers.

14. All bearer bonds, letters of credit, money drafts, money orders, cashier's checks, travelers checks, Treasury checks, bank checks, passbooks, bank drafts, money wrappers, stored value cards, and other forms of financial remuneration evidencing the obtaining, secreting, transfer, and/or concealment of assets and/or expenditures of money;

15. All Western Union and/or Money Gram documents and other documents evidencing domestic or international wire transfers, money orders, official checks, cashier's checks, or other negotiable interests that can be purchased with cash, to include applications, payment records, money orders, frequent customer cards, etc;

16. Negotiable instruments, jewelry, precious metals, financial instruments, and other negotiable instruments;

17. Documents reflecting the source, receipt, transfer, control, ownership, and disposition of United States and/or foreign currency;

18. Correspondence, papers, records, and any other items showing employment or lack of employment;

19. Telephone books, and/or address books, facsimile machines, any papers reflecting names, addresses, telephone numbers, pager numbers, cellular telephone numbers, facsimile, and/or telex numbers, telephone records and bills relating to co-conspirators, sources of supply, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists. Also, telephone answering devices that record telephone conversations and the tapes therein for messages left for or by co-

1 conspirators for the delivery or purchase of controlled substances or laundering of drug  
2 proceeds;

3 20. Safes and locked storage containers, and the contents thereof which are  
4 otherwise described in this document;

5 21. Tools: Tools that may be used to open hidden compartments in vehicles,  
6 paint, bonding agents, magnets, or other items that may be used to open/close said  
7 compartments;

8 22. Any and all mailing documents and packaging materials related to U.S.  
9 Postal Service to include USPS Express Mail labels, express mail and priority envelopes,  
10 first class mailings, receipts for USPS packages, and tracking information;

11 23. Any records or information pertaining to the dark web and dark web  
12 marketplaces, including the Empire Market.

13 24. Any records or information pertaining to the Subject Moniker (or spelling  
14 variants thereof);

15 25. Cryptocurrency applications and wallets, to include information regarding  
16 current account balance and transaction history, i.e., date, time, amount, an address of the  
17 sender/recipient of a cryptocurrency transaction maintained in such wallets;

18 26. Any records or information reflecting cryptocurrencies, including web  
19 history, and documents showing the location, source, and timing of acquisition of any  
20 cryptocurrencies, to include wallets, wallet addresses, and seed phrases;

21 27. Any evidence of cryptocurrency ownership or usage, to include the  
22 following: (a) any and all representations of cryptocurrency public keys or addresses,  
23 whether in electronic or physical format; (b) any and all representations of  
24 cryptocurrency private keys, whether in electronic or physical format; and (c) any and all  
25 representations of cryptocurrency wallets or their constitutive parts, whether in electronic  
26 or physical format, to include "recovery seeds" and "root keys" which may be used to  
27 regenerate a wallet.

28 28. Cell Phones: Cellular telephones and other communications devices may be  
seized, and searched for the following items:

- a. Assigned number and identifying telephone serial number (ESN, MIN,  
IMSI, or IMEI);



- b. Stored list of recent received, sent, and missed calls;
- c. Stored contact information;
- d. Stored photographs of narcotics, currency, firearms or other weapons, evidence of suspected criminal activity, and/or the user of the phone and/or co-conspirators, including any embedded GPS data associated with these photographs;
- e. Stored text messages, as well as any messages in any internet messaging apps, including but not limited to Facebook Messenger, iMessage, Wickr, Telegram, Signal, WhatsApp, Kik, and similar messaging applications, related to the aforementioned crimes of investigation or that may show the user of the phone and/or co-conspirators, including Apple iMessages, Blackberry Messenger messages or other similar messaging services where the data is stored on the telephone;
- f. Any Tor applications and records for Tor activity, including browser history and “bookmarked” or “favorite” web pages;
- g. Digital currency applications and wallets, to include information regarding current account balance and transaction history, i.e., date, time, amount, an address of the sender/recipient of a digital currency transaction maintained in such wallets;
- h. Stored documents, notes, and files that contain passwords/or encryption keys;
- i. PGP applications, to include stored private and/or public keys;
- j. Any records or information related to the use of the Subject Moniker (or spelling variants thereof); and

29. Digital devices, such as computers, and other electronic storage media, such as USBs and Trezor devices, may be seized, and searched for the following items:

- a. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,



browsing history, user profiles, e-mail, e-mail contacts, "chats," instant messaging logs, photographs, and correspondence;

- b. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
- c. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
- d. Evidence of the times the digital device or other electronic storage media was used;
- e. Passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;
- f. Contextual information necessary to understand the evidence described in this attachment;
- g. Records or information pertaining to the dark web and dark web marketplaces, including the Empire Market.
- h. Any records or information pertaining to the Subject Moniker (or spelling variants thereof);
- i. Any records or information pertaining to Tor;
- j. Any records or information pertaining to mnemonic phrases;
- k. Any records or information reflecting cryptocurrencies, including web history, and documents showing the location, source, and timing of acquisition of any cryptocurrencies, to include wallets, wallet addresses, and seed phrases;
- l. Any records or information pertaining to PGP applications, to include private and/or public keys;

THE SEIZURE OF DIGITAL DEVICES IS AUTHORIZED FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATION OF THEIR CONTENTS FOR

1 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED  
2 CRIMES  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28